

# **BlackBerry Smart Card Reader**

Version 2.0

**Security Technical Overview** 

## Contents

BlackBerry Smart Card Reader	4
Authenticating a user using a smart card	4
Integrating a smart card with existing secure messaging technology	4
New in this release	5
System requirements	6
System architecture	7
BlackBerry Enterprise Solution security	8
Protecting Bluetooth connections on a BlackBerry device	8
Managing a Bluetooth enabled BlackBerry device	8
Restricting Bluetooth technology on a Bluetooth enabled computer	9
Bluetooth security measures on the BlackBerry Smart Card Reader	9
BlackBerry Smart Card Reader security	10
Control Bluetooth connections from third-party applications	11
Managing the BlackBerry Smart Card Reader	12
Opening an encrypted and authenticated connection to the BlackBerry Smart Card Reader	14
Secure pairing PIN	14
Performing the Bluetooth pairing process and the secure pairing process on a BlackBerry device.	15
Performing the Bluetooth pairing process and the secure pairing process on a computer	15
Reconnecting to a BlackBerry device or computer automatically	15
Initial key establishment protocol used in the secure pairing process	15
Connection key establishment protocol used in the secure pairing process	16
Encrypting and authenticating data on the application layer	18
Two-factor authentication	18
Turning on two-factor authentication on a BlackBerry device	18
Configuring two-factor authentication on a computer	19
Proximity authentication	20
Locking a BlackBerry device when the BlackBerry Smart Card Reader moves out of Bluetooth technology range	20
Configuring a BlackBerry device to use a specific BlackBerry Smart Card Reader	20
Two-factor content protection	20
Process flow: Protecting the content encryption key using two-factor content protection	21
BlackBerry Smart Card Reader supported algorithms	22
Connection key establishment protocol errors	23
Application layer protocol encryption and authentication	24

BlackBerry Smart Card Reader shared cryptosystem parameters	25
Examples of attacks that the BlackBerry Smart Card Reader security protocols are designed to prevent	26
Eavesdropping	26
Impersonating a BlackBerry device or computer	26
Man-in-the-middle attack	26
Offline attack	26
Offline dictionary attack	27
Online dictionary attack	27
Small subgroup attack	27
Smart card binding information	28
BlackBerry Smart Card Reader reset process	29
Related resources	30
Glossary	31
Provide feedback	32
Legal notice	33

### BlackBerry Smart Card Reader

The BlackBerry® Smart Card Reader is an accessory that, when used in proximity to certain Bluetooth® enabled BlackBerry devices and computers, permits users to authenticate with their smart cards and log in to Bluetooth enabled BlackBerry devices and computers.

The BlackBerry Smart Card Reader is designed to perform the following actions:

- communicate with Bluetooth enabled BlackBerry devices and computers using Bluetooth technology version 1.1 and later and using the AES-256 encryption method (by default) on the application layer
- create a reliable two-factor authentication environment for granting users access to the PKI applications on BlackBerry devices and computers
- enable the wireless digital signing and encryption of wireless email messages sent from the BlackBerry device using the S/MIME Support Package for BlackBerry® smartphones
- store all encryption keys in RAM only and never write the keys to flash memory

### Authenticating a user using a smart card

The BlackBerry® Smart Card Reader permits you to use two-factor authentication, using a smart card, to require users to prove their identities to the BlackBerry devices or computers by two factors:

- what they have (the smart card)
- what they know (their smart card password)

### Integrating a smart card with existing secure messaging technology

In addition to standard BlackBerry® encryption, you can extend secure messaging technology to offer an additional layer of security between the sender and the recipient of an email or PIN message. The S/MIME Support Package for BlackBerry® smartphones is designed so that users who send and receive S/MIME messages using their email applications can send and receive S/MIME protected messages using their BlackBerry devices. Users can sign, encrypt, and send S/MIME protected messages from their BlackBerry devices. BlackBerry devices can decrypt S/MIME-encrypted messages that they receive so that users can read the messages on their BlackBerry devices.

To pair Bluetooth® enabled BlackBerry devices with the BlackBerry® Smart Card Reader, users must install a smart card driver, the BlackBerry Smart Card Reader driver on their BlackBerry devices, and, optionally, a smart card authenticator module. The S/MIME Support Package for BlackBerry smartphones supports smart card use and includes tools that users can use to download certificates and transfer them to the BlackBerry device for use with the S/MIME Support Package for BlackBerry smartphones.

After the BlackBerry device and the BlackBerry Smart Card Reader establish a secure pairing, you can configure the S/MIME Force Smartcard Use IT policy rule to require the use of the smart card to sign, encrypt, or sign and encrypt S/MIME-protected messages on the BlackBerry device.

## New in this release

Feature	Description
proximity authentication	Proximity authentication is an authentication method that permits a user to unlock a BlackBerry® device using a BlackBerry device password and a BlackBerry® Smart Card Reader when the BlackBerry Smart Card Reader is located within Bluetooth® technology range of the BlackBerry device. Proximity authentication does not require the user to have a smart card.
two-factor content protection	Two-factor content protection requires a BlackBerry device password, a smart card, and an authentication certificate that is stored on a BlackBerry device to protect the content protection key.
configuration of a secure pairing PIN	You can configure the length of a secure pairing PIN and use alphanumeric characters in the secure pairing PIN.

# System requirements

The BlackBerry® Smart Card Reader supports the following software and BlackBerry devices:

Bla	ckBerry Enterprise Server software	Computer	BlackBerry devices
•	BlackBerry® Enterprise Server version 4.0 SP2 and later for Microsoft® Exchange (with the S/MIME IT Policy Pack imported)	Windows® XP SP2 or SP3 (32- bit and 64-bit versions) with support for Bluetooth® technology turned on	Java® based Bluetooth enabled BlackBerry devices that run BlackBerry® Device Software version 4.1 and later
•	BlackBerry Enterprise Server version 4.0 SP3 or later	<ul> <li>Windows Vista™ (32-bit and 64-bit versions) with support for Bluetooth technology turned on</li> </ul>	

## System architecture

The BlackBerry® Smart Card Reader is designed to connect to a Bluetooth® enabled BlackBerry device and a Bluetooth enabled computer. The BlackBerry Smart Card Reader supports using certificates that a PKI generates with a BlackBerry device.

The BlackBerry Smart Card Reader cannot communicate with the BlackBerry® Enterprise Server directly. When the BlackBerry device pushes an IT policy to the BlackBerry Smart Card Reader, the BlackBerry Smart Card Reader preserves the BlackBerry Enterprise Server signature on the IT policy.

### **BlackBerry Enterprise Solution security**

The BlackBerry® Enterprise Solution is designed to encrypt data that is in transit at all points between a BlackBerry device and the BlackBerry® Enterprise Server to help protect your organization from data loss or alteration. Only the BlackBerry Enterprise Server and the BlackBerry device can decrypt the data that they send between each other. If events that threaten the wireless security of your organization occur, the BlackBerry Enterprise Solution is designed to prevent third parties, including wireless service providers, from accessing potentially sensitive information in a decrypted format.

The BlackBerry Enterprise Solution uses symmetric key cryptography to encrypt messages and data that it sends over the transport layer.

### Protecting Bluetooth connections on a BlackBerry device

Bluetooth® technology permits a Bluetooth enabled BlackBerry® device to open a wireless connection with other Bluetooth devices that are within a 10-meter range (for example, a hands-free car kit or wireless headset).

A Bluetooth profile on the BlackBerry device specifies how applications can connect and run. The Bluetooth Serial Port Profile on the BlackBerry device specifies how the BlackBerry device can open a serial connection to another Bluetooth enabled device using a virtual serial port.

By default, a BlackBerry device that is running BlackBerry® Device Software version 4.0 and later includes the following security measures:

- You or a user can turn off the Bluetooth technology for the BlackBerry device.
- The user must request a connection or pairing on the BlackBerry device with another Bluetooth device. The user must also type a shared secret key (called a passkey) to complete the pairing.
- The user can specify whether to encrypt data to and from the BlackBerry device over a Bluetooth connection. The BlackBerry® Enterprise Solution uses the passkey to generate encryption keys.
- The BlackBerry device prompts the user each time a Bluetooth device tries to connect to the BlackBerry device.

### Managing a Bluetooth enabled BlackBerry device

Using BlackBerry® Enterprise Server version 4.0 and later, you can use IT policy rules to manage the Bluetooth® technology on a Bluetooth enabled BlackBerry device. For example, you can use IT policies to configure the following behavior:

- prevent the BlackBerry device from opening a Bluetooth connection to another Bluetooth enabled BlackBerry device, another Bluetooth enabled device, or the BlackBerry® Desktop Software
- prevent a user from turning on Discoverable mode on the BlackBerry device
- require the BlackBerry device to use Bluetooth encryption on all connections
- require the BlackBerry device to prompt the user to type the BlackBerry device password to turn on Bluetooth support
- require the BlackBerry device to prompt the user to type the BlackBerry device password to turn on discoverable mode
- prevent the BlackBerry device from using the Bluetooth Headset Profile, the Bluetooth Handsfree Profile, or the Bluetooth Serial Port Profile
- prevent the BlackBerry device from bypassing the wireless network over a Bluetooth connection
- prevent the BlackBerry device from sending or receiving contact list information over a Bluetooth connection
- prevent the BlackBerry device from making phone calls

For more information, see the *BlackBerry Enterprise Server Policy Reference Guide*.

### Restricting Bluetooth technology on a Bluetooth enabled computer

On a Bluetooth® enabled computer, when a Bluetooth wireless adaptor exists and is turned on, the computer also installs Bluetooth drivers (and a personal area networking device, optionally) for that wireless adaptor. To prevent a user who does not have administrator privileges and external Bluetooth devices other than the BlackBerry® Smart Card Reader from using the Bluetooth technology installed on the computer, you can restrict the availability of the Bluetooth technology on the computer.

For more information about restricting Bluetooth technology on a computer in your organization, see *Restricting Bluetooth technology on Bluetooth enabled computers BlackBerry Smart Card Reader Technical Overview.* 

# Bluetooth security measures on the BlackBerry Smart Card Reader

The following security methods on the BlackBerry® Smart Card Reader enhance the existing protection of the Bluetooth® technology on a Bluetooth enabled BlackBerry device.

Security method	Description
limited use of serial port profiles	The BlackBerry Smart Card Reader uses the Bluetooth Serial Port Profile only, allowing you to use application control to turn off all the other profiles and prevent third-party applications from using the BlackBerry Smart Card Reader.
use of Bluetooth pairing process to help prevent passive attack	During the Bluetooth pairing process, the BlackBerry Smart Card Reader uses a random key (unlike the hard-coded keys that headsets and other Bluetooth enabled devices use).
	A user always starts the Bluetooth pairing process from the BlackBerry device or computer. If a message prompts the user to type a pairing password when the user did not start a pairing process, the user knows that another device, which the user might not want to connect to, started the pairing process. The Bluetooth pairing process is designed to help prevent a passive attack in which a user with malicious intent tries to search for the BlackBerry device PIN.
control of the Bluetooth range	You can use the Maximum Bluetooth Range IT policy rule to control the power level of the Bluetooth wireless adapter on the BlackBerry Smart Card Reader. When you configure the power level, you can control the range of proximity between the BlackBerry Smart Card Reader and the BlackBerry device at which the two parties close the Bluetooth connection between them. The range value does not translate to a specific distance because the Bluetooth range is partially determined by the power level. The range value is also heavily influenced by environmental factors, including obstructions and electromagnetic radiation. As a general rule, the Bluetooth range at power setting <i>n</i> +1 is longer than the range at power setting <i>n</i> .
protection of the Bluetooth encryption key	After the user resets the BlackBerry Smart Card Reader, a BlackBerry device can perform the Bluetooth pairing process and the secure paring process to reconnect to the BlackBerry Smart Card Reader. If that BlackBerry device was the last BlackBerry device to connect to the BlackBerry Smart Card Reader before the user reset the BlackBerry Smart Card Reader, the BlackBerry Smart Card Reader restores the backed-up Bluetooth encryption key for that Bluetooth connection and opens the Bluetooth connection to the BlackBerry device automatically. You can use the Maximum Bluetooth Encryption Key Regeneration Period IT policy rule to set the period after which the BlackBerry device generates a new Bluetooth encryption key.

# **BlackBerry Smart Card Reader security**

The BlackBerry® Smart Card Reader is designed to prevent offline and online dictionary attacks using the following security methods.

Security method	Description
authentication of connections	The BlackBerry Smart Card Reader uses processes designed to perform the following actions:
	pair the BlackBerry Smart Card Reader with a Bluetooth® enabled BlackBerry device or Bluetooth enabled computer using a Bluetooth encryption key to open a Bluetooth connection between them
	<ul> <li>pair the smart card with the BlackBerry device or computer using a secure pairing PIN, which is created the first time that the BlackBerry Smart Card Reader pairs with the BlackBerry device or computer, to open an authenticated connection between them</li> </ul>
	generate session keys to help protect data that the BlackBerry device or computer and the BlackBerry Smart Card Reader send between them on the application layer over the Bluetooth connection
deletion of connection information	A BlackBerry device that is connected to the BlackBerry Smart Card Reader can delete the secure pairing PIN when the BlackBerry device disconnects from the BlackBerry Smart Card Reader and the disconnection timeout period expires.
	A computer that is connected to the BlackBerry Smart Card Reader can delete the secure pairing PIN when the computer enters standby mode.
shared device transport key	The BlackBerry Smart Card Reader creates a shared private key and then creates a shared device transport key from the secure pairing PIN and a secret private key.
BlackBerry Smart Card Reader password	The first BlackBerry device or computer to connect to the BlackBerry Smart Card Reader after the BlackBerry Smart Card Reader resets must create the BlackBerry Smart Card Reader password. This password helps protects the encryption keys on the BlackBerry Smart Card Reader in the same way that the BlackBerry device password protects the data on the BlackBerry device.
	Any debugging application that tries to connect to the BlackBerry Smart Card Reader over the USB connection cannot connect unless that application knows the password.
	After ten unsuccessful password tries, the BlackBerry Smart Card Reader deletes all its data, including the password.
protected key storage	To help limit the risk of key disclosure, the BlackBerry Smart Card Reader is designed to store all keys in its RAM only and does not write keys to its flash memory. To take the BlackBerry Smart Card Reader apart, the user must remove the battery. When the user removes the battery, the BlackBerry Smart Card Reader deletes all the keys.
	A BlackBerry device that runs BlackBerry® Device Software version 4.1 and later and a computer store the current secure pairing PIN and the shared device transport key in their respective RAM only. A BlackBerry device that runs BlackBerry Device Software versions earlier than version 4.1 stores the secure pairing PIN and the shared device transport key in a key store database in the flash memory.

Security method	Description
code signing	Before a user can run a permitted third-party application that uses the controlled APIs on the BlackBerry device, the Research In Motion signing authority system must use public key cryptography to authorize and authenticate the application code.  The BlackBerry Smart Card Reader uses code signing to prevent the user from loading third-party code onto the BlackBerry Smart Card Reader. When RIM manufactures the BlackBerry Smart Card Reader, it installs a public key into the secure boot ROM of the BlackBerry Smart Card Reader and uses the corresponding private key to sign the BlackBerry Smart Card Reader operating system. When RIM loads an operating system and BlackBerry Java® Virtual Machine onto the BlackBerry Smart Card Reader, the boot ROM verifies the signature on the loaded operating system. If the boot ROM determines that the signature is not valid, it rejects the operating system.  See the BlackBerry Enterprise Solution Security Technical Overview for more information about code signing.
random number generation	<ul> <li>In the BlackBerry Smart Card Reader, the following sources of entropy seed the random number generator:</li> <li>RIM manufactures each BlackBerry Smart Card Reader with a random 64-byte value (a seed). This provides the BlackBerry Smart Card Reader with entropy before the wireless adapter is turned on.</li> </ul>
	<ul> <li>When the initial key establishment protocol generates the device transport key and the connection key establishment protocol generates the connection key that the BlackBerry device or computer and the BlackBerry Smart Card Reader use to send data between them, the BlackBerry device or computer and the BlackBerry Smart Card Reader use SHA-512 to hash all the data packets that they send and receive between them and add the hashed data packets to the entropy pool.</li> </ul>
	<ul> <li>Each time the BlackBerry device or computer and the BlackBerry Smart Card Reader negotiate keys during the initial key establishment protocol and the connection key establishment protocol, the BlackBerry device or computer sends a 64-byte seed to the BlackBerry Smart Card Reader. The BlackBerry Smart Card Reader adds this value to its random source.</li> </ul>
	See the <i>BlackBerry Enterprise Solution Security Technical Overview</i> for more information about the process for random number generation on the BlackBerry device.

For more information, see "BlackBerry Smart Card Reader reset process".

### Control Bluetooth connections from third-party applications

Application control is designed to limit the use of Bluetooth® technology (and the Bluetooth profiles) to specific, permitted third-party applications. Using the BlackBerry® Enterprise Server version 4.0 and later, you can configure IT policy rules and application policy rules to control how third-party applications use the BlackBerry® Smart Card Reader to connect to a Bluetooth enabled BlackBerry device.

Use application control policy rules to control the following behavior on the BlackBerry device:

- permit or prevent a user from downloading third-party applications
- define the features (for example, the email application, the phone application, and the BlackBerry device key store) that third-party applications can access
- define the types of connections that a third-party application can open (for example, opening network connections inside the firewall)
- send third-party applications to the BlackBerry device over the wireless network

• prevent third-party applications that have obtained a digital signature from the Research In Motion signing authority system from using the BlackBerry device controlled APIs to do anything other than access persistent storage of user data and communicate with other applications

You can configure application control policy rules so that all Bluetooth profiles are unavailable for applications by default and then turn on the Bluetooth Serial Port Profile for the BlackBerry Smart Card Reader driver only. In this configuration, only the necessary applications are allowed to use the BlackBerry Smart Card Reader driver.

### Managing the BlackBerry Smart Card Reader

You can configure IT policy rules to manage the behavior of the BlackBerry® Smart Card Reader.

IT policy rule	Description
Disable Auto Reconnect To BlackBerry Smart Card Reader	This rule prevents automatic reconnections to the BlackBerry Smart Card Reader from a previously connected BlackBerry device and computer.
	Turning off automatic reconnections from the BlackBerry device is designed to increase the life of battery on the BlackBerry device.
Force Erase All Keys on BlackBerry Disconnected Timeout	This rule specifies whether a BlackBerry device deletes its secure pairing PIN and closes its connection to the BlackBerry Smart Card Reader when the connection timeout period expires.
	This rule also specifies whether the BlackBerry Smart Card Reader deletes all secure pairing PINs and closes all connections to a connected computer when the connection timeout period expires.
Force Erase Key On PC Standby	This rule specifies whether a computer deletes its secure pairing PIN and closes the connection to the BlackBerry Smart Card Reader when the computer enters standby mode.
Force Smart Card Two Factor Authentication	This rule specifies whether a user must type the BlackBerry device password and the smart card password to use a BlackBerry device.
	You can use Windows® Local Security Policy settings to specify whether a user must connect to a supported smart card reader from the Windows login screen to use a computer.
Force Smart Card Two Factor Challenge Response	This rule specifies whether a user must choose a smart card certificate for use with smart card two-factor authentication. If two-factor authentication is turned on, when the user unlocks a BlackBerry device, the BlackBerry device sends a challenge to the smart card to verify that it is the same smart card that the BlackBerry device used to initialize the smart card authenticator module.
Lock on Smart Card Removal	This rule specifies whether a BlackBerry device locks when a user removes the smart card from a smart card reader or disconnects a smart card reader from the BlackBerry device. If you want to use this rule, you must verify that the smart card reader driver that your organization uses supports smart card removal detection.
	You can use Windows Local Security Policy settings to specify whether a computer locks when the user removes the smart card from a smart card reader or disconnects a smart card reader from the computer.
Maximum Bluetooth Encryption Key Regeneration Period	This rule specifies a period, in hours, after which the BlackBerry Smart Card Reader regenerates a Bluetooth® encryption key if a BlackBerry device or computer is connected to the BlackBerry Smart Card Reader when the period expires. If the BlackBerry device or computer is not connected to the BlackBerry Smart Card Reader when the period expires, the BlackBerry Smart Card Reader regenerates the Bluetooth encryption key when the BlackBerry device or computer reconnects to the BlackBerry Smart Card Reader.

IT policy rule	Description
Maximum Connection Heartbeat Period	This rule specifies the maximum heartbeat period, in seconds. During each heartbeat period, the paired BlackBerry device or computer sends a heartbeat, which the BlackBerry Smart Card Reader acknowledges. If either side does not send or acknowledge a heartbeat in the maximum heartbeat period, the BlackBerry device or computer closes the Bluetooth connection. When the Bluetooth connection closes, the disconnected timer starts if you or the user turned that feature on for the BlackBerry device or computer. The BlackBerry device or computer deletes the secure pairing PINs when the disconnected timer expires. You can use this IT policy rule to help prevent a user with malicious
	intent from using a low-level Bluetooth heartbeat to perform the following actions:
	keep the Bluetooth connection open between the BlackBerry device or computer and the BlackBerry Smart Card Reader
	keep the secure pairing PINs present for an extended period after the BlackBerry device and BlackBerry Smart Card Reader should close the Bluetooth connection
Maximum BlackBerry Disconnected Timeout	This rule specifies the maximum time, in seconds, after a BlackBerry device and the BlackBerry Smart Card Reader close the Bluetooth connection between them that the disconnection timeout period expires.
	You can use the Force Erase All Keys on BlackBerry Disconnected Timeout IT policy rule to specify whether the BlackBerry device or computer delete the secure pairing PINs for the current connection to the BlackBerry Smart Card Reader when the disconnection timeout period expires.
Maximum BlackBerry Long Term Timeout	This rule specifies the maximum time, in hours, after the BlackBerry device and the BlackBerry Smart Card Reader open the secure pairing connection between them that the BlackBerry device and the BlackBerry Smart Card Reader delete the secure pairing information.
Maximum BlackBerry Bluetooth Traffic Inactivity Timeout	This rule specifies the maximum time, in minutes, of inactivity over a Bluetooth connection between the BlackBerry Smart Card Reader and a BlackBerry device that the BlackBerry device and the BlackBerry Smart Card Reader wait before deleting the secure pairing information.
Maximum Smart Card Not Present Timeout	This rule specifies the maximum time, in seconds, after a user removes the smart card from the BlackBerry Smart Card Reader that the secure pairing information is deleted from a BlackBerry device and the BlackBerry Smart Card Reader.
Maximum Number of BlackBerry Transactions	This rule specifies the maximum number of transactions (smart card-related operations) that a BlackBerry device and the BlackBerry Smart Card Reader can send and receive before the secure pairing information is deleted from the BlackBerry device.
Maximum Bluetooth Range	This rule specifies the maximum power range, as a value between 30% (the shortest range) and 100% (the longest range), that the BlackBerry Smart Card Reader can use to send Bluetooth data packets.
Maximum PC Disconnected Timeout	This rule specifies the maximum time, in seconds, after a computer and the BlackBerry Smart Card Reader close the Bluetooth connection between them that the secure pairing information for the closed connection is deleted from the computer and the BlackBerry Smart Card Reader.

IT policy rule	Description
Maximum PC Long Term Timeout	This rule specifies the maximum time, in hours, after a computer and the BlackBerry Smart Card Reader open the secure pairing connection between them that the computer and the BlackBerry Smart Card Reader delete the secure pairing information.
Maximum PC Bluetooth Traffic Inactivity Timeout	This rule specifies the maximum time, in minutes, of inactivity over the Bluetooth connection between the BlackBerry Smart Card Reader and a computer before the computer and the BlackBerry Smart Card Reader delete the secure pairing information.
Maximum Number of PC Transactions	This rule specifies the maximum number of transactions (smart card related operations) that a computer and the BlackBerry Smart Card Reader can send and receive between them before the computer and the BlackBerry Smart Card Reader delete the secure pairing information.
	A transaction is any request and response set of data packets other than a connection heartbeat.
Maximum Number of PC Pairings	This rule specifies the maximum number of computers that can pair with the BlackBerry Smart Card Reader.

The BlackBerry Smart Card Reader also uses the Disable Radio When Cradled IT policy rule, which controls whether the wireless adapter is turned off when the BlackBerry device is connected to USB peripherals. If you change this rule to Yes, the Bluetooth wireless adaptor of the BlackBerry Smart Card Reader is turned off whenever the BlackBerry Smart Card Reader is connected to a computer using a USB connection.

For more information. see the BlackBerry Enterprise Server Policy Reference Guide.

# Opening an encrypted and authenticated connection to the BlackBerry Smart Card Reader

Before the BlackBerry® Smart Card Reader and a BlackBerry device or computer can open an encrypted and authenticated connection between them, the BlackBerry Smart Card Reader and the BlackBerry device or computer must perform a Bluetooth® pairing process to open a Bluetooth connection. The BlackBerry Smart Card Reader and the BlackBerry device or computer can then perform a secure pairing process to open a connection between the smart card and the BlackBerry device or computer. The secure pairing process is designed to allow the BlackBerry Smart Card Reader and the BlackBerry device or computer to encrypt and authenticate the data that they send between them over the application layer.

During the secure pairing process the following events occur:

- the initial key establishment protocol creates a shared device transport key on the BlackBerry device or computer and the BlackBerry Smart Card Reader that the BlackBerry device or computer and the BlackBerry Smart Card Reader use to encrypt and decrypt the data that they send between them
- the connection key establishment protocol creates a shared connection key on the BlackBerry device or computer and the BlackBerry Smart Card Reader that the BlackBerry device or computer and the BlackBerry Smart Card Reader use to send data between them

The user must perform a Bluetooth pairing process once only but must perform a secure pairing each time that the BlackBerry device or computer deletes the secure pairing information. You can control when the BlackBerry device or computer deletes the secure pairing information using BlackBerry Enterprise Server IT policy rules for the BlackBerry Smart Card Reader.

#### Secure pairing PIN

The first time that the BlackBerry® Smart Card Reader connects to a BlackBerry device or computer, the BlackBerry Smart Card Reader pairs with the BlackBerry device or computer using Bluetooth® technology and generates a secure pairing PIN. The secure pairing PIN is designed to protect data as it travels between the BlackBerry Smart

Card Reader and the BlackBerry device or computer. By default, the secure pairing PIN is 8 characters long and is case-sensitive.

If your organization uses BlackBerry Smart Card Reader version 2.0 and later and BlackBerry® Device Software version 5.0 and later, you can change the length of the secure pairing PIN using the Minimum PIN Entry Mode IT policy rule. BlackBerry Smart Card Reader version 2.0 and later and BlackBerry Device Software version 5.0 and later support alphanumeric characters.

# Performing the Bluetooth pairing process and the secure pairing process on a BlackBerry device

A user can start a Bluetooth® pairing process and a secure pairing process by clicking Connect on the BlackBerry® Smart Card Reader options screen on a BlackBerry device. If the user is running BlackBerry® Device Software version 4.0 and later on the BlackBerry device, the user can start the secure pairing process by trying an action on the BlackBerry device that requires the smart card (for example, importing certificates, signing or decrypting a message, or turning on two-factor authentication). If the user is running BlackBerry Device Software version 4.0.2 and later on the BlackBerry device, trying an action on the BlackBerry device that requires the smart card can also start the Bluetooth pairing process.

For more information, see the BlackBerry Smart Card Reader Getting Started Guide.

### Performing the Bluetooth pairing process and the secure pairing process on a computer

A user must manually connect to the BlackBerry® Smart Card Reader from the BlackBerry Smart Card Reader Options dialog box on the computer to start the Bluetooth® pairing process. When the Bluetooth pairing is established, the computer automatically prompts the user to perform the secure pairing process.

For more information see the BlackBerry Smart Card Reader Getting Started Guide.

### Reconnecting to a BlackBerry device or computer automatically

The BlackBerry® Smart Card Reader is designed to reconnect automatically to a BlackBerry device or computer that it has previously connected with and if it has not deleted the Bluetooth® encryption key or secure pairing PIN. You can configure the Disable Auto Reconnect To BlackBerry Smart Card Reader IT policy rule to prevent the BlackBerry Smart Card Reader from reconnecting to the BlackBerry device or computer automatically. Turning off the automatic reconnection feature is designed to increase the battery life of the BlackBerry device.

#### Initial key establishment protocol used in the secure pairing process

The initial key establishment protocol uses the ECDH algorithm to negotiate numerous algorithms that are used in subsequent secure pairing PIN and connection key exchanges, including the following algorithms:

- the elliptic curve used by future ECDH exchanges
- the encryption algorithm and hash algorithms used by the encryption and authentication processes on the application layer

The initial key establishment protocol is designed to use 521-bit Random Curve. The initial key establishment protocol is designed to negotiate to use AES-256 and SHA-256 for application layer encryption and authentication, and SHA-512 for IT policy authentication.

For more information, see "BlackBerry Smart Card Reader supported algorithms".

### Initial key establishment protocol process

- 1. The BlackBerry® device or computer sends an initial echo of the value 0xC1F34151520CC9C2 to the BlackBerry® Smart Card Reader to confirm that a Bluetooth® connection to the BlackBerry Smart Card Reader exists and to verify that both sides understand the protocol.
- 2. The BlackBerry Smart Card Reader receives the initial echo and replies with an echo transmission of the same value.
- **3.** The BlackBerry device or computer receives the echo and replies to the BlackBerry Smart Card Reader with a request for a list of supported algorithms.

- **4.** The BlackBerry Smart Card Reader creates a list of all the algorithms that it supports and sends the supported algorithms list to the BlackBerry device or computer.
- 5. The BlackBerry device or computer searches the list for a match with one of its own supported algorithms.
  - If a match is not available, the BlackBerry device or computer sends an error to the BlackBerry Smart Card Reader and stops processing the list.
  - If a match exists, the BlackBerry device or computer begins the key establishment process by sending
    a pairing request using the selected algorithms and a 64-byte seed to the BlackBerry Smart Card
    Reader.
- **6.** The BlackBerry Smart Card Reader verifies the selected algorithms.
- 7. The BlackBerry Smart Card Reader performs the following calculation to select a short-term key (Y):
  - selects random y, 1 < y < r 1
  - calculates Y = yS
- **8.** The BlackBerry Smart Card Reader sends Y to the BlackBerry device or computer.
- **9.** The BlackBerry device or computer performs the following calculations to select a short-term key (X):
  - selects random x, 1 < x < r 1
  - calculates X = xS
  - calculates the device transport key (*MK*) using the following information:

Parameter	Value
K	xY = xyS
H1	SHA-512 (sent data packets)
H2	SHA-512 (received data packets)

- calculates H = H1 + H2
- calculates MK = SHA-256( H || K)
- **10.** The BlackBerry device sends *X* to the BlackBerry Smart Card Reader.
- 11. The BlackBerry Smart Card Reader calculates *MK* using the following information:

Parameter	Value
K	yX = yxS
H1	SHA-512 (sent data packets)
H2	SHA-512 (received data packets)
Н	H1 + H2
MK	SHA-256 ( <i>H</i>    <i>K</i> )

The BlackBerry device or computer and the BlackBerry Smart Card Reader share a device transport key.

For more information about variables used in this process, see "BlackBerry Smart Card Reader shared cryptosystem parameters".

### Connection key establishment protocol used in the secure pairing process

After the initial key establishment protocol process completes successfully, a BlackBerry® device or computer and the BlackBerry® Smart Card Reader share a device transport key. They must then generate a connection key to use to send data between them. The connection key establishment protocol starts from the secure pairing PIN s using SPEKE, letting the BlackBerry device or computer generate long-term public keys and a strong, cryptographically protected connection with the BlackBerry Smart Card Reader.

The connection key establishment protocol uses the ECDH algorithm that the initial key establishment protocol negotiates. The ECDH algorithm provides Perfect Forward Secrecy, which uses the key that protects data to prevent the protocol from deriving previous or subsequent encryption keys. Each run of the connection key establishment protocol uses a unique, random, ephemeral key pair to create the new connection key. The BlackBerry Smart Card Reader discards the ephemeral key pair after generating the connection key. Even if the ephemeral private keys from a particular protocol run using the ECDH algorithm are compromised, the connection keys from other runs of the same protocol remain uncompromised.

### Connection key establishment protocol process

- 1. The BlackBerry® device or computer sends an initial echo of the value 0xC1F34151520CC9C2 to the BlackBerry® Smart Card Reader to confirm that a Bluetooth® connection to the BlackBerry Smart Card Reader exists and to verify that both sides understand the protocol.
- 2. The BlackBerry Smart Card Reader receives the initial echo and replies with an echo transmission of the same value.
- 3. The BlackBerry device or computer receives the echo and uses the algorithm that the initial key establishment protocol negotiated to send the selected algorithms and a seed to the BlackBerry Smart Card Reader.
- 4. The BlackBerry Smart Card Reader performs the following calculation to select a short-term key (Y):
  - selects random y, 1 < y < r − 1</li>
  - calculates Y = yP
  - where *P* is defined on the curve negotiated by the initial key establishment protocol
- **5.** The BlackBerry Smart Card Reader sends Y to the BlackBerry device or computer.
- **6.** The BlackBerry device or computer performs the following calculation to select a short-term key (X):
  - selects random x, 1 < x < r 1
  - calculates X = xP
  - calculates the connection key (*CK*) using the following information:

Parameter	Value	
K	Y = xyP	
H1	SHA-512 (sent data packets)	
H2	SHA-512 (received data packets)	
Н	H1 + H2	
CK	SHA-256 ( <i>MK</i>    <i>H</i>    <i>MK</i>    <i>K</i> )	

- **7.** The BlackBerry device or computer sends X to the BlackBerry Smart Card Reader.
- **8.** The BlackBerry device or computer performs a hashing function to calculate CK.
- **9.** The BlackBerry Smart Card Reader calculates CK using the following information:

Parameter	Value Value	
K	yX = yxP	
H1	HA-512 (sent data packets)	
H2	SHA-512 (received data packets)	
Н	H1 + H2	
CK	SHA-256( <i>MK</i>    <i>H</i>    <i>MK</i>    <i>K</i> )	

The BlackBerry device or computer and the BlackBerry Smart Card Reader share a connection key.

For more information about variables used in this process, see "BlackBerry Smart Card Reader shared cryptosystem parameters".

The connection key establishment protocol can stop at any point if an error occurs. For more information, see "Connection key establishment protocol errors".

### Encrypting and authenticating data on the application layer

When a BlackBerry® device or a computer and the BlackBerry® Smart Card Reader complete the secure pairing process, all data that they send between them is encrypted and authenticated on the application layer by keys that they derive from the shared connection key. By default, the BlackBerry device or computer and the BlackBerry Smart Card Reader use AES 256 in CBC mode to encrypt the data and keyed HMAC with SHA-512 to protect data, but they can negotiate different algorithms during the initial key establishment protocol.

The keys protect the data on the application layer throughout the entire connection. A lost or closed connection occurs if either the BlackBerry device or the BlackBerry Smart Card Reader goes outside of the Bluetooth® technology range or if the BlackBerry device wireless adapter or the computer's Bluetooth adapter turns off for any reason. When a Bluetooth connection closes, if the BlackBerry device or computer's Bluetooth connection to the BlackBerry Smart Card Reader is lost, they must renegotiate the keys.

You can configure the Maximum Connection Heartbeat Period IT policy rule to control when the Bluetooth connection closes based on the secure heartbeat settings. For more information about configuring this IT policy rule, see "Managing the BlackBerry Smart Card Reader".

For more information, see "Application layer protocol encryption and authentication".

### Two-factor authentication

If a user has a smart card authenticator module, smart card driver, and smart card reader driver installed on a BlackBerry® device or computer, you or the user can start the process for two-factor authentication on the BlackBerry device or computer. The process is designed to bind the BlackBerry device or computer to the installed smart card. After the BlackBerry device or computer binds to the smart card, it requires that smart card to authenticate the user.

### Turning on two-factor authentication on a BlackBerry device

You can configure the Force Smart Card Two-Factor Authentication IT policy rule to require that a user uses a smart card to authenticate with a BlackBerry® device. If you do not force the user to use a smart card to authenticate with the BlackBerry device, the user can turn on or turn off two-factor authentication with the smart card by changing the User Authenticator field in the Security options on the BlackBerry device.

When you turn on two-factor authentication on the BlackBerry device, the following events occur:

- The BlackBerry device locks.
- The BlackBerry device pushes the current IT policy to the BlackBerry® Smart Card Reader.
- When a user tries to unlock the BlackBerry device, the BlackBerry device prompts the user to type the BlackBerry device password. If the user has not yet set a BlackBerry device password, the BlackBerry device forces the user to set a password.
- The BlackBerry device prompts the user to type the smart card password to turn on two-factor authentication with the installed smart card.
- The BlackBerry device binds to the installed smart card automatically by storing the smart card binding information in a BlackBerry device NV store, which is designed to be inaccessible to the user.

When a user turns on two-factor authentication on the BlackBerry device, the following events occur:

- The BlackBerry device prompts the user to type the BlackBerry device password. If the user has not yet configured a BlackBerry device password, the BlackBerry device forces the user to set a password.
- The BlackBerry device prompts the user to type the smart card password to turn on two-factor authentication with the installed smart card.

• The BlackBerry device binds to the installed smart card automatically by storing the smart card binding information in a BlackBerry device NV store location, which is designed to be inaccessible to the user.

For more information, see "Smart card binding information".

#### Confirming that a BlackBerry device is bound to the correct smart card

After a user turns on two-factor authentication, whenever a BlackBerry® device prompts the user to insert the smart card into the BlackBerry® Smart Card Reader, the BlackBerry device prompt indicates the label and the card type of the correct (bound) smart card.

The user can also view smart card information in the Security options on the BlackBerry device.

Field	Description	
Name	This field indicates the type of the installed smart card.	
Initialized	This field indicates whether the BlackBerry device is authenticated with and bound to the smart card	
	A value of Yes indicates that the BlackBerry device is bound to the smart card.	
	A value of No indicates that the BlackBerry device is not bound to the smart card.	

### Unbinding the smart card from a BlackBerry device

When you or a user start the process that permits a BlackBerry® device to permanently deletes its stored user and application data, the BlackBerry device deletes the smart card binding information from its NV store. When the process completes, a user can authenticate with the BlackBerry device using a new smart card.

You can delete the smart card binding information from the BlackBerry device manually in the following ways:

- Send the Erase Data and Disable Device IT administration command to the BlackBerry device to delete the binding between a user's current smart card and the BlackBerry device.
- When the user turns off two-factor authentication, the BlackBerry device turns off two-factor authentication with the installed smart card and deletes the smart card binding information from the BlackBerry device.

### Configuring two-factor authentication on a computer

For information about configuring a computer to require the user to connect to a supported smart card reader from the Windows login screen to use the computer, see the Windows® documentation.

### **Proximity authentication**

Proximity authentication is an authentication method that permits a user to unlock a BlackBerry® device using the BlackBerry device password and the BlackBerry® Smart Card Reader within Bluetooth® technology range of the BlackBerry device. To unlock a BlackBerry device, the user moves the BlackBerry Smart Card Reader within Bluetooth technology range of the BlackBerry device, clicks the unlock button on the BlackBerry device, and types the BlackBerry device password. Proximity authentication does not require the user to use a smart card.

By default, if you or a user turns on proximity authentication and the user does not move the BlackBerry Smart Card Reader within Bluetooth technology range, the user can unlock the BlackBerry device using the BlackBerry device password. To require a user to use proximity authentication, you must change the value of the Allowed Authentication Mechanisms IT policy rule to Proximity.

BlackBerry® Device Software version 5.0 and later and BlackBerry Smart Card Reader version 2.0 and later support proximity authentication. You must verify that the IT policies that you can use to manage proximity authentication are available on your organization's BlackBerry® Enterprise Server. BlackBerry Enterprise Server version 5.0 SP1 and later includes the IT policies that you require to manage proximity authentication.

You cannot use proximity authentication to log in to a Bluetooth enabled computer.

# Locking a BlackBerry device when the BlackBerry Smart Card Reader moves out of Bluetooth technology range

If your organization uses proximity authentication, you or a user can configure a BlackBerry® device to lock when a user moves the BlackBerry® Smart Card Reader out of Bluetooth® technology range. If you or a user configures this option, the BlackBerry device closes the Bluetooth connection to the BlackBerry Smart Card Reader and locks when the user moves out of Bluetooth technology range. To make this option mandatory, you must change the Lock on Proximity Authenticator Disconnect IT policy rule to Yes. When you change this rule to Yes, the user cannot change the option on the BlackBerry device.

### Configuring a BlackBerry device to use a specific BlackBerry Smart Card Reader

You can use the password options on a BlackBerry® device to configure a specific BlackBerry® Smart Card Reader with a BlackBerry device. You or a user can configure proximity authentication so that the user cannot change the BlackBerry Smart Card Reader that the user uses to unlock the BlackBerry device. When you or the user configures a specific BlackBerry Smart Card Reader with the BlackBerry device, a user with malicious intent cannot use another BlackBerry Smart Card Reader to unlock the BlackBerry device and access data. If the battery power level for a specific BlackBerry Smart Card Reader that you or a user configures with a BlackBerry device is empty, the user cannot unlock the BlackBerry device until the user recharges the battery.

For more information, see the online help on the BlackBerry device.

### Two-factor content protection

Content protection is designed to encrypt data on a BlackBerry® device when the BlackBerry device is locked. When you configure two-factor content protection, the content encryption key encrypts the user data on the BlackBerry device, the BlackBerry device generates a key using the BlackBerry device password that encrypts the content encryption key, and the private key that is stored on the smart card encrypts the key that the BlackBerry device generates. When you configure two-factor content protection, the content encryption key is not transferred from the BlackBerry device to the BlackBerry® Smart Card Reader.

Two-factor content protection requires the BlackBerry device password, a smart card, and an authentication certificate that is stored on the BlackBerry device. The authentication certificate must contain the public key for the private key that is stored on the smart card. If the authentication certificate expires or is revoked before a user can replace it, the user must delete all BlackBerry device data from the BlackBerry device before the BlackBerry device can recover. This feature is designed to protect the user data on the BlackBerry device if the BlackBerry device is lost or stolen.

You or a user can configure two-factor content protection. By default, if a user has a smart card and an authentication certificate on the BlackBerry device, the user can turn on two-factor content protection. To make two-

factor content protection mandatory or optional, or to prevent a user from configuring it, you can use the Two-factor Content Protection Usage IT policy rule. After you or a user turns on two-factor content protection, to unlock the BlackBerry device, a user must type the BlackBerry device password and the smart card PIN on the login screen in the appropriate fields.

If you or a user turns on two-factor content protection, you cannot change the BlackBerry device password using the BlackBerry Administration Service. Only the user can change the BlackBerry device password on the BlackBerry device.

BlackBerry® Device Software version 5.0 and later and BlackBerry® Smart Card Reader version 2.0 and later support two-factor content protection. You must verify that the IT policies that you can use to manage two-factor content protection are available on your organization's BlackBerry® Enterprise Server. BlackBerry Enterprise Server version 5.0 SP1 and later includes the IT policies that you require to manage two-factor content protection.

### Process flow: Protecting the content encryption key using two-factor content protection

- 1. You or a user turns on two-factor content protection.
- 2. The BlackBerry® device performs the following actions:
  - a. generates a random 256-bit secret key for the smart card authenticator module
  - b. uses the secret key for the smart card authenticator module and the BlackBerry device password to generate a 256-bit ephemeral key
    - The BlackBerry device encrypts the ECC private key and content protection key using the ephemeral key, and stores the keys in the BlackBerry device memory.
  - c. generates a 256-bit pseudorandom number
  - d. computes the SHA-256 hash of the pseudorandom number and uses it to encrypt the secret key
    for the smart card authenticator module, and stores the secret key in the BlackBerry device
    memory
  - e. encrypts the pseudorandom number using the public key in the certificate that you configured for use with two-factor content protection, and stores the public key in the BlackBerry device memory
  - f. discards the pseudorandom number, SHA-256 hash of the pseudorandom number, ephemeral key, and key for the smart card user authenticator module after it completes the protection process for the ECC private key and content protection key
- **3.** When the BlackBerry device locks, the BlackBerry device discards the ECC private key and content protection key.
- **4.** When a user unlocks the BlackBerry device, the BlackBerry device retrieves the encrypted copy of the pseudorandom number from the BlackBerry device memory and sends it to the smart card authenticator.
- **5.** The smart card authenticator decrypts the encrypted copy of the pseudorandom number that was stored in the BlackBerry device memory.
- **6.** The BlackBerry device performs the following actions:
  - a. retrieves the encrypted copy of the key for the smart card authenticator module from the BlackBerry device memory and decrypts it using the SHA-256 hash of the pseudorandom number
  - b. uses the key for the smart card authenticator module and the BlackBerry device password to generate a 256-bit ephemeral key
  - c. uses the 256-bit ephemeral key to decrypt the ECC private key and content protection key
  - d. repeats steps 2c to 2f

The BlackBerry device generates a new pseudorandom number each time the user unlocks the BlackBerry device.

For more information about how the content protection key protects user data, see the *BlackBerry Enterprise Solution Security Technical Overview*.

# BlackBerry Smart Card Reader supported algorithms

Algorithm type	Algorithm	
elliptic curve	571-bit Koblitz Curve (EC571K1)	
(default)	521-bit Random Curve (EC521R1)	
	283-bit Koblitz Curve (EC283K1)	
	256-bit Random Curve (EC256R1)	
	160-bit Random Curve (EC160R1)	
	The initial key establishment protocol is designed to negotiate to use the 521-bit Random Curve (EC521R1) algorithm unless the BlackBerry® device or the computer requires a different algorithm.	
encryption	AES-256 (default)	
	• AES-128	
	The initial key establishment protocol is designed to negotiate to use the AES-256 algorithm unless the BlackBerry device or the computer requires a different algorithm.	
hash	• SHA-512	
	• SHA-256	
	• SHA-1	
	The initial key establishment protocol is designed to negotiate to use SHA-512 or SHA-256 algorithm unless the BlackBerry device or the computer requires a different algorithm.	

## Connection key establishment protocol errors

During the connection key establishment protocol process, if an error occurs on the BlackBerry® device, the computer, or the BlackBerry® Smart Card Reader, that party sends an error code to the other party negotiating the connection key. The following errors might occur:

- negative length
- bad packet
- incomplete crypto specification
- bad public key
- no algorithms in common are permitted
- not paired
- not connected
- connection error
- decryption error

## Application layer protocol encryption and authentication

By default, each data packet that a BlackBerry® device or computer and the BlackBerry® Smart Card Reader send between them is authenticated and encrypted using the following methods:

- authenticated with HMAC using the negotiated SHA algorithm
- encrypted with AES of the negotiated key size using CBC mode

The following diagram shows the anatomy of a data packet formatted for transmission over the application layer:

4 bytes	8 bytes	4 bytes	Variable	Based on SHA	Variable	
IV	Random padding	Counter	Payload	HMAC-SHA	PKC5 padding	

Area authenticated by HMAC

Area encrypted with AES-256

The connection key protocol opens a shared connection key *CK* from which the BlackBerry device or computer and the BlackBerry Smart Card Reader derive the four session keys that they use on the application layer to protect the data that they send between them.

Connection session key	Value	Description
KeySendEnc	SHA-256( <i>CK</i>    <i>S</i> 1)	This key is the AES-256 key that the BlackBerry device, the computer, or the BlackBerry Smart Card Reader generates to encrypt the data that it sends to the other party over the application layer.
		The other party must use KeyRecEnc to respond to KeySendEnc.
KeyRecEnc	SHA-256( <i>CK</i>    <i>S2</i> )	This key is the AES-256 key that the BlackBerry device, the computer, or the BlackBerry Smart Card Reader generates to decrypt the data that it receives from the other party over the application layer.
KeySendAuth	SHA-256( <i>CK</i>    <i>S3</i> )	This key is the HMAC authentication key that the BlackBerry device, the computer, or the BlackBerry Smart Card Reader generates to authenticate the data that it sends to the other party over the application layer.
		The other party must use KeyRecAuth to respond to KeySendAuth.
KeyRecAuth	SHA-256( <i>CK</i>    <i>S4</i> )	This key is the HMAC authentication key that the BlackBerry device, the computer, or the BlackBerry Smart Card Reader generates to authenticate the data that it receives from the other party over the application layer.

**Note**: *S1*, *S2*, *S3*, and *S4* are hard-coded strings that the BlackBerry device or computer and the BlackBerry Smart Card Reader use in the key derivation to prevent calculating session keys that are the same as each other.

# BlackBerry Smart Card Reader shared cryptosystem parameters

The BlackBerry® Smart Card Reader and a BlackBerry device or computer with the BlackBerry Smart Card Reader software and drivers installed are designed to share the following cryptosystem parameters.

Parameter	Description	
E(Fq)	This parameter is the NIST-approved 521-bit random elliptic curve over Fq, which has a cofactor of 1.	
	The initial establishment key protocol performs all mathematical operations in the group E(Fq).	
Fq	This parameter is a finite field of prime order q.	
Р	This parameter is a point of E that generates a subgroup of E(Fq) of prime order r.	
xR	This parameter is a representation of elliptic curve scalar multiplication, where x is the scalar and R is a point on E(Fq).	
S	This parameter is the secure pairing PIN value that appears in the BlackBerry Smart Card Rea window.	
	The secure pairing PIN must be known only to the authorized user of the BlackBerry device or computer and the BlackBerry Smart Card Reader until the protocol completes.	
S	This parameter is the secure pairing value (s) converted to a point on E(Fq).	

# Examples of attacks that the BlackBerry Smart Card Reader security protocols are designed to prevent

### **Eavesdropping**

An eavesdropping event occurs when a user with malicious intent listens to the communication between the BlackBerry® Smart Card Reader and a BlackBerry device or computer. The goal of the user with malicious intent is to determine the shared device transport key on the BlackBerry Smart Card Reader and the BlackBerry device or computer, given only xS and yS.

The initial key establishment protocol and the connection key establishment protocol are designed so that the user with malicious intent can only compute the device transport key by solving the ECDH problem. This calculation is equivalent to solving the DH problem, which is considered computationally infeasible.

### Impersonating a BlackBerry device or computer

An impersonation of the BlackBerry® Smart Card Reader occurs when a user with malicious intent sends messages to a BlackBerry device or computer so that the BlackBerry device or computer believes it is communicating with the BlackBerry Smart Card Reader. The user with malicious intent must send X = xP, instead of xS to the BlackBerry Smart Card Reader. A user with malicious intent might try this when the user with malicious intent does not know the secure pairing PIN.

The initial key establishment protocol is designed so that the BlackBerry Smart Card Reader calculates K = yX = yxP. To calculate the same key, the user with malicious intent must determine y from Y. This problem is considered to be computationally infeasible.

The connection key establishment protocol is designed so that a user with malicious intent can perform only the following actions:

- quess the secure pairing PIN
- compute the device transport key by solving the discrete log problem, which is computationally infeasible, to try to determine the secret private key on the BlackBerry device or computer

### Man-in-the-middle attack

A man-in-the-middle attack occurs when a user with malicious intent intercepts and modifies messages in transit between the BlackBerry® Smart Card Reader and a BlackBerry device or computer. A successful man-in-the-middle attack results in each party not knowing that the user with malicious intent is sitting between them, monitoring and changing data traffic.

The user with malicious intent must remain in the middle (between the BlackBerry device or computer and the BlackBerry Smart Card Reader) forever, not just for the duration of the key establishment protocol, for a man-in-the-middle attack to occur. For a user with malicious intent to successfully start a man-in-the-middle attack, the user with malicious intent must know the secure pairing PIN.

The initial key establishment protocol is designed to use ECDH and the shared device transport key to prevent a man-in-the-middle attack. If the user with malicious intent learns the secure pairing PIN after the initial key establishment protocol is complete, the mathematical difficulty of the discrete log problem protects the device transport key. To determine the device transport key, the user with malicious intent must determine one of *x* or *y*. The user cannot gain knowledge of the device transport key before the initial key establishment protocol begins as long as the secure pairing PIN remains secret until the initial key establishment protocol completes successfully.

The connection key establishment protocol is designed to use SPEKE to prevent a man-in-the-middle attack through the use of the secure pairing PIN.

### Offline attack

An offline attack occurs when a user with malicious intent tries to send X = xP, instead of xS to the BlackBerry® Smart Card Reader. The user with malicious intent might try this when the user with malicious intent does not know the secure pairing PIN. The initial key establishment protocol is designed so that the BlackBerry Smart Card Reader replies with Y=xS and calculates K = yX = yxP. Meanwhile, the user with malicious intent must calculates K = xY = yxP.

yxS = yxzP, for some z such that S = zP. To calculate yxP from yzxP without knowledge of z corresponds to solving the discrete logarithm problem, which is computationally infeasible, for S.

### Offline dictionary attack

An offline dictionary attack occurs when a user with malicious intent tries all possible passwords and determines the correct password. The connection key establishment protocol is designed to use SPEKE to prevent a known offline dictionary attack through the use of a password (the secure pairing PIN) in case the user with malicious intent uses computational resources (where, in theory, nothing limits the speed at which the user with malicious intent can force the password) to determine the password.

### Online dictionary attack

An online dictionary attack is similar to an offline dictionary attack, but a user with malicious intent must rely on the BlackBerry® device, the computer, or the BlackBerry® Smart Card Reader to determine if a key is the correct secure pairing PIN.

The BlackBerry Smart Card Reader supports only one try to guess the secure pairing PIN. If the guess is incorrect, the BlackBerry Smart Card Reader changes the secure pairing PIN before the next try occurs.

### Small subgroup attack

A small subgroup attack occurs when a user with malicious intent tries to limit the protocol to generate device transport keys from only a small subset of keys.

The BlackBerry® Smart Card Reader security protocols are designed to use ECDH operations that use a cofactor in their calculations and verify that the result is not the point at infinity. For example, if the user with malicious intent chooses X as the point at infinity, then K is the point at infinity regardless of what the BlackBerry Smart Card Reader chose for Y. By checking that X is not at the point of infinity, 1, or -1, the BlackBerry Smart Card Reader security protocols are designed to avert this threat.

### Smart card binding information

When you or a user turns on two-factor authentication on a BlackBerry® device, the BlackBerry device binds to the installed smart card automatically by storing the following smart card binding information in a special BlackBerry device NV store location that is inaccessible to a user:

- the name of a Java® class that the BlackBerry® Smart Card Reader requires
- the binding information format
- the smart card type (for the Common Access Card, this string is "GSA CAC")
- the name of a Java class that the smart card code requires
- a unique 64-bit identifier that the smart card provides
- a smart card label that the smart card provides (for example, "AIME.ANDREA.1234567890")

**Note**: If the BlackBerry device uses a challenge/response certificate, the binding information format is a version byte with a value of 1. If the BlackBerry device does not use a challenge/response certificate, the binding information format is a version byte with a value of 0.

### BlackBerry Smart Card Reader reset process

When a user resets the BlackBerry® Smart Card Reader, the BlackBerry Smart Card Reader performs the following actions:

- backs up the Bluetooth® encryption key for the currently connected BlackBerry device, if applicable
- deletes all Bluetooth pairing information
- deletes all secure pairing information
- deletes all user settings
- deletes the connection password
- unbinds the IT policy from the BlackBerry Smart Card Reader

The BlackBerry Smart Card Reader unbinds the IT policy by deleting the IT policy public key from the NV store so that it can receive a new IT policy and digitally signed IT policy public key from a BlackBerry® Enterprise Server. The BlackBerry Smart Card Reader does not delete the stored IT policy.

## Related resources

Resource	Information
BlackBerry Enterprise Solution Security Technical Overview	<ul> <li>preventing the decryption of information at an intermediate point between the BlackBerry® device and the BlackBerry® Enterprise Server or organization LAN</li> </ul>
	managing security settings for all BlackBerry devices
	protecting data that is in transit between the BlackBerry device and the BlackBerry Enterprise Server
	<ul> <li>understanding the algorithms provided by the RIM Cryptographic API</li> </ul>
	understanding the TLS and WTLS standards that the RIM Cryptographic API currently supports
	understanding the process that occurs to securely delete data on the BlackBerry device when content protection feature is turned on
BlackBerry Enterprise Server	generating and changing device transport keys
Administration Guide	turning on S/MIME protected messaging
	turning on encryption options
	setting IT policy rules
	setting message classifications
BlackBerry Smart Card Reader Getting	setting up the BlackBerry® Smart Card Reader
Started Guide	installing or upgrading the BlackBerry Smart Card Reader
	pairing the BlackBerry device or the computer with the BlackBerry Smart Card Reader
	troubleshooting
BlackBerry Enterprise Server Policy Reference Guide	understanding BlackBerry Enterprise Server IT policy rules and application control policy rules
	using IT policies and application control policies
S/MIME Support Package User Guide Supplement	<ul> <li>installing the S/MIME Support Package for BlackBerry® smartphones</li> </ul>
	managing certificates on the BlackBerry device and computer
	specifying S/MIME options for digitally signing and encrypting messages
	sending and receiving S/MIME protected messages
Security for BlackBerry devices with	understanding Bluetooth® technology
Bluetooth Wireless Technology	understanding the risks of using Bluetooth technology on mobile devices
	protecting Bluetooth enabled BlackBerry devices
Visit www.blackberry.com/security.	information about BlackBerry® Enterprise Solution security

### **Glossary**

#### **AES**

Advanced Encryption Standard

#### API

application programming interface

### CBC

cipher block chaining

### **ECDH**

Elliptic Curve Diffie-Hellman

### **HMAC**

keyed-hash message authentication code

### LAN

local area network

### LED

light-emitting diode

### NIST

National Institute of Standards and Technology

### NV

nonvolatile

#### PIN

personal identification number

#### PKI

Public Key Infrastructure

### S/MIME

Secure Multipurpose Internet Mail Extensions

### SHA

Secure Hash Algorithm

### **SPEKE**

Simple Password-authenticated Exponential Key Exchange

### TLS

Transport Layer Security

#### **WTLS**

Wireless Transport Layer Security

## Provide feedback

To provide feedback on this deliverable, visit  $\underline{\text{www.blackberry.com/docsfeedback}}.$ 

### Legal notice

#### Document ID: 25979072 version 3

©2009 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, SureType®, SurePress™ and related trademarks, names, and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world.

Bluetooth is a trademark of Bluetooth SIG. Java is a trademark of Sun Microsystems, Inc. Microsoft, Windows, and Windows Vista are trademarks of Microsoft Corporation. All other brands, product names, company names, trademarks and service marks are the properties of their respective owners.

The BlackBerry smartphone and other devices and/or associated software are protected by copyright, international treaties, and various patents, including one or more of the following U.S. patents: 6,278,442; 6,271,605; 6,219,694; 6,075,470; 6,073,318; D445,428; D433,460; D416,256. Other patents are registered or pending in the U.S. and in various countries around the world. Visit www.rim.com/patents for a list of RIM (as hereinafter defined) patents.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available at www.blackberry.com/go/docs is provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by Research In Motion Limited and its affiliated companies ("RIM") and RIM assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect RIM proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of RIM technology in generalized terms. RIM reserves the right to periodically change information that is contained in this documentation; however, RIM makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party web sites (collectively the "Third Party Products and Services"). RIM does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by RIM of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NONINFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL RIM BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NONPERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH RIM PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF RIM PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, RIM SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO RIM AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED RIM DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF RIM OR ANY AFFILIATES OF RIM HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with RIM's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You

should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with RIM's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by RIM and RIM assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with RIM.

Certain features outlined in this documentation require a minimum version of BlackBerry® Enterprise Server, BlackBerry® Desktop Software, and/or BlackBerry® Device Software.

The terms of use of any RIM product or service are set out in a separate license or other agreement with RIM applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY RIM FOR PORTIONS OF ANY RIM PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

Certain features outlined in this documentation might require additional development or Third Party Products and Services for access to corporate applications.

This product contains a modified version of HTML Tidy. Copyright © 1998-2003 World Wide Web Consortium (Massachusetts Institute of Technology, European Research Consortium for Informatics and Mathematics, Keio University). All Rights Reserved.

This product includes software developed by the Apache Software Foundation (www.apache.org/) and/or is licensed pursuant to one of the licenses listed at (www.apache.org/licenses/). For more information, see the NOTICE.txt file included with the software.

Research In Motion Limited

295 Phillip Street

Waterloo, ON N2L 3W8

Canada

Research In Motion UK Limited

Centrum House

36 Station Road

Egham, Surrey TW20 9LF

United Kingdom

Published in Canada